Remote Access Policy

1.0 Purpose
The purpose of this policy is to define standards for connecting to the Judiciary's network from any host. These standards are designed to minimize the potential exposure to the Judiciary from damages which may result from unauthorized use of Judicial resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Judicial internal systems, etc.

2.0 Scope
This policy applies to all Judicial employees, contractors, vendors and agents with a Judicial-owned or personally-owned computer or workstation used to connect to the Judicial network. This policy applies to remote access connections used to do work on behalf of the Judiciary, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy
3.1 General
1. It is the responsibility of Judicial employees, contractors, vendors and agents with remote access privileges to the Judiciary's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Judicial network.
2. Family members of Judicial employees are not permitted to access network resources of the Judiciary. The Judicial employee is responsible to ensure a family member does not access any Judicial network resources, and does not perform illegal activities. The Judicial employee bares responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of the Judiciary's network:
    a. *Virtual Private Network (VPN) Policy*
    b. *Acceptable Use Policy*

3.2 Requirements
1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication, RSA token, or public/private keys with strong pass-phrases.
2. At no time should any Judicial employee provide their login or email password to anyone, not even family members.
3. Judicial employees and contractors with remote access privileges must ensure that their Judicial-owned or personal computer or workstation, which is remotely connected to the Judiciary's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Judicial employees and contractors with remote access privileges to the Judiciary's network must not use non-Judicial email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Judicial business, thereby ensuring that official business is never confused with personal business.
5. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. Non-standard hardware configurations must be approved by Remote Access Services, and information technology staff must approve security configurations for access to hardware.
7. All hosts that are connected to the Judicial network via remote access technologies must use the most up-to-date anti-virus software (http://www.symantec.com), this includes personal computers.
8. Personal equipment that is used to connect to the Judiciary's network must meet the requirements of Judicial-owned equipment for remote access.

9. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Judicial production network must obtain prior approval from the Director of Judicial Information Systems for access to Supreme Court resources, or the Director of the Court of Appeals Information Technology department for access to COA resources.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Cable Modem:	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
Dial-in Modem:	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing:	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Judicial network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Judicial-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into the Judicial network and an ISP, depending on packet destination.
DSL:	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Remote Access:	Any access to the Judiciary's corporate network through a non-Judicial controlled network, device, or medium.
Split-tunneling:	Simultaneous direct access to a non-Judicial network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into the Judiciary's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.
Judicial Network:	Any network resource of the Michigan Supreme Court or Court of Appeals.

6.0 Revision History

_____ _____
Signature Date